Verizon Scam Alert Advisory

The Delaware State Police is providing a Scam Alert Advisory. This is a general alert which covers any part of the State of Delaware.

The Delaware State Police have recently received a complaint from a citizen in Kent County concerning a phone call from an individual stating they are with Verizon. The person claiming to be from Verizon said the network was switching from 4G to 5G and the service would experience issues in the next few days. The caller claimed, in order to avoid issues with service, an account reset is needed. The victim received a password reset email and provided the confirmation code to the caller to reset the account. The caller then instructed the victim to turn off the cell phone to complete the account reset and network update. The victim turned the cell phone on and moments later received another email from Verizon confirming his order for an Apple Ipad tablet. The order was made in the victim's name and was set to be shipped. Verizon was notified of the incident.

Taking steps to prevent identity theft can greatly reduce the chances of becoming a victim. Below are a few suggestions for protecting yourself online and offline.

- Shred all documents containing Personally Identifying Information such as your Social Security Number, your credit card or account numbers, even your middle name. This can include bank or credit card statements, preapproval letters, or utility bills. If you aren't sure, shred it before discarding it. Use locked filing cabinet or a document safe for important documents that you want to keep.
- Protect all of your online passwords. Don't store them on paper or in unsecured files.
- Be cautious when showing personally identifying

information on social media sites.

- Be wary of callers that are providing you information on your account and then ask you to provide basic account information.
- Validate promotional offers with the company before logging into your online account to accept them. For example, if you get an email promising a \$30 bill credit of your wireless bill, do some research online to see if it's a scam. When in doubt, contact the company directly to validate the offer.
- Secure your internet connection. Using public wifi connections may place you at risk for a fraudster to obtain the information stored on your computer or smartphone.
- Regularly monitor your credit report for unusual or unauthorized activity. Many sites offer a free credit report for a promise to subscribe to additional services. Under the Fair Credit Act, you are entitled to a free credit report from the reporting agencies.

Information provided through the Verizon website located at: https://www.verizonwireless.com/fraud/

For more information on identity theft, please visit www.consumer.ftc.gov/topics/privacy-identity

Anyone with information in reference to this incident is asked to please contact Troop 4, Detective Powell at 302-856-5850. Information may also be provided by calling Delaware crime stoppers at 1-800-TIP-3333 or via the internet at http://www.delaware.crimestoppersweb.com

Many of these scams are difficult to investigate. They will target persons of all age groups. Delaware State Police is asking citizens to remember the tips previously mentioned in order to not become a victim of one of these scam artists.

You can follow the Delaware State Police by clicking on:

Delaware State Police Official Web Site

Facebook

<u>Twitter</u>

<u>Nextdoor</u>

Please tell us how we're doing via our <u>Citizen Satisfaction</u> <u>Survey</u>.

Presented by the Director of Public Information, Sergeant Richard Bratz,

Released: 120818 2255

-End-